

Appl. No. : 09/965,968
Filed : September 26, 2001

SUMMARY OF INTERVIEW

Exhibits and/or Demonstrations

None

Identification of Claims Discussed

Claim 13 was discussed.

Identification of Prior Art Discussed

The prior art reference to Groshon was discussed, as well as the references to Blickenstaff and Korn.

Proposed Amendments

None

Principal Arguments and Other Matters

Applicant argued that Groshon does not teach or suggest a public web server and a private web server with a firewall to provide protection for the private web server. Applicant further argued that Groshon does not teach or suggest that the public web server sends requests for web content to the private web server when the public web server determines that the web content has been corrupted, and that the private web server provides encrypted content to the public web server.

Results of Interview

Applicant agreed to file a response to the outstanding office action with the above arguments.

Appl. No. : 09/965,968
Filed : September 26, 2001

REMARKS

The foregoing amendments are responsive to the February 16, 2006 Office Action. Applicant respectfully request reconsideration of the present application in view of the foregoing amendments and the following remarks.

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Response to Objection to Claim 13

The Examiner objected to informalities in Claim 13. Applicant has amended Claim 13 to correct the informalities identified by the Examiner and to correct spelling error not identified by the Examiner. This amendment corrects typographical errors and do not add new matter.

In view of the amendments, Applicant requests the Examiner to withdraw the objection to Claim 13.

Response to Rejection of Claims 13 and 15-16 Under 35 U.S.C. 103(a)

The Examiner rejected Claims 13 and 15-16 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,351,811 to Groshon et al. ("Groshon"), in view of European Patent No. 467,239 to Bianco, and further in view of U.S. Patent No. 5,537,585 to Blickenstaff et al. (Blickenstaff) and U.S. Patent No. 6,880,083 to Korn.

Groshon teaches a system wherein a digital signature associated with requested data is compared to a control signature. However, in Groshon the web page data is not protected by being encrypted. Further, in Groshon the backup web page storage is not protected from an attacker. In Groshon (see, e.g., Fig 10), the backup web page storage is directly available to the public web server and, thus, available to be modified by an attacker. Thus, Groshon does not teach or suggest the level of protection for web content claimed by Applicant.

By contrast, in Applicant's system the web content stored on the public server is protected by being encrypted. The backup web content is protected from attack because it is not directly accessible from the public server and, thus, not accessible by an attacker. The backup web content is provided to a private server which is separated from the public server by a firewall. When unauthorized modification of the encrypted content on the public web server is detected, the encrypted copy can be restored by sending a request to the protected private server. No combination

of Groshon with the other references teaches such a system wherein the public content is protected by encryption and the private content is protected behind a firewall.

Blickenstaff teaches a data system wherein low priority data files are migrated via the network and the storage server to backend data storage media. Thus, Blickenstaff teaches a backup-type system. However, Blickenstaff does not teach or suggest protection of private web content as described above.

Korn teaches a process for executing a script on a user's computer (see Fig 2). Korn does not teach or suggest a method to allow a website server to detect that the web content has been altered. The teachings of Korn do not suggest recovery of website content from a private server because Korn teaches giving a warning to the end user rather than to the website server. Thus, Korn does not teach or suggest the claimed invention because Korn teaches detection of a problem at the wrong place and at the wrong time.

Bianco teaches a method for encryption, but does not teach or suggest how to use such encryption to protect web content.

Applicant respectfully submits that the Examiner is using hindsight in making the rejection. "The genius of invention is often a combination of known elements which in hindsight seems preordained. To prevent hindsight invalidation of patent claims, the law requires some 'teaching, suggestion or reason' to combine cited references." *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 60 USPQ2d 1001 (Fed. Cir. 2001). "Consequently, the tests of whether to combine references need to be applied rigorously." *Id.* "In making the assessment of differences, section 103 specifically requires consideration of the claimed invention; as a whole." *Ruiz v. A.B. Chance Co.*, 357 F.3d 1270, 69 USPQ2d 1686 (Fed. Cir. 2004). "This form of hindsight reasoning, using the invention as a roadmap to find its prior art components, would discount the value of combining various existing features or principles in a new way to achieve a new result – often the very definition of invention." *Id.* In the present case, the Examiner has used Applicant's disclosure as a roadmap to find prior art components. The prior art contains no suggestion or teaching to combine elements to produce the claimed invention.

Further evidence of non-obviousness is found in the fact that the BitShield Corp 3GWeb-I-2400 product, which is based on the claimed invention, was a "2005 Best of Interop" award winner (as disclosed in the Office Action Response filed July 21, 2005 in response to the first Office Action). The award was based in part on "[h]ow the product advances the state of the art

Appl. No. : **09/965,968**
Filed : **September 26, 2001**

for networking" (*See e.g.*, *Litton Systems, Inc. v. Honeywell, Inc.* 87 F.3d 1559, 39 USPQ2d 1321 (Fed. Cir. 1996) (tributes from others of skill in the art as evidence of non-obviousness.)

Regarding Claim 13, the cited prior art does not teach or suggest an anti-alteration system for web-content having a public-web-server configured to create safe-web-files encrypted from original web-content including one or more types of static files and one or more types of dynamic files, and configured to provide HTTP web server functions, a private-web-server configured to provide the original web-content the public-web-server provided to the private-web-server through a firewall, wherein when a web visitor's request is received, the public-web-server is configured to verify that the safe-web-file has not been improperly altered, deleted or replaced, the public-web-server further configured to decrypt one or more of the safe-web-files and respond to the visitor, and the public-web-server further configured to automatically send a recovery request to the private-web-server when the public-web-server detects an unauthorized alteration of the safe-web-files, the private-web-server, in response to the recovery request, configured to send the safe-web-files to the public server.

Regarding Claim 15, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 13, further comprising a real-time-check module used on the public-web-server computer for linking to a decryption module, wherein the decryption module is configured to decrypt one or more of the safe-web-files in response to an HTTP request received from the web visitor.

Regarding Claim 16, the cited prior art does not teach or suggest the anti-alteration system as recited in Claim 15, further comprising a real-time-check module configured to use symmetric-key encryption to decrypt one or more of the safe-web-files when the web visitor's request is received.

Accordingly, Applicant asserts that Claims 13 and 15-16 are allowable over the prior art, and Applicant requests allowance of Claim 13 and 15-16.

Response to Rejection of Claim 14 Under 35 U.S.C. 103(a)

The Examiner rejected Claim 14 under 35 U.S.C. 103(a) as being unpatentable over the modified Scott, Groshon et al., Bianco, and Blickenstaff et al. system as applied to Claim 1 above, further in view of Menezes et al. (*Handbook of Applied Cryptography*) and further in view of Thomson (U.S. Patent No. 5,276,874).

As described above, Groshon teaches a system wherein a digital signature associated with requested data is compared to a control signature. However, in Groshon the web page data is not

Appl. No. : **09/965,968**
Filed : **September 26, 2001**

protected by being encrypted. Further, in Groshon the backup web page storage is not protected from an attacker. In Groshon, the backup web page storage is directly available to the web server and, thus, available to be modified by an attacker.

By contrast, in Applicant's system the web content stored on the public server is protected by being encrypted. The backup web content is protected from attack because it is not directly accessible from the public server and, thus, not accessible by an attacker. The backup web content is provided to a private server which is separated from the public server by a firewall. When unauthorized modification of the encrypted content on the public web server is detected, then the encrypted copy can be restored by sending a request to the protected private server. No combination of Groshon with Bianco and Blickenstaff and Menezes teaches such a system wherein the public content is protected by encryption and the private content is protected behind a firewall.

Applicants respectfully submit that the Examiner's rejection is based on hindsight.

Regarding Claim 14, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 13, wherein the encryption comprises chaos encryption technology to do encryption and decryption of the web-content for increasing the web server response speed and increasing security strong of whole system.

Response to Rejection of Claims 17-28 Under 35 U.S.C. 103(a)

The Examiner rejected Claims 17-28 under 35 U.S.C. 103(a) as being unpatentable over the modified Scott, Groshon et al., Bianco, and Blickenstaff et al. system as applied to Claim 1 above, further in view of Menezes et al. (Handbook of Applied Cryptography) and further in view of Thomson. As discussed above in connection with Claim 1, the cited art does not teach or suggest the claimed invention.

Regarding Claim 17, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 16, wherein the symmetric-key encryption is selected from a group consisting essentially of DES, 3DES and AES.

Regarding Claim 18, the cited prior art does not teach or suggest an anti-alteration system for web-content having a public-web-server configured to store safe-web-contents that have been provided with header information including a MAC (Message Authentication Code) generated from the original web-content, and properties of the original-web-content including, name, size, date, and location thereof, a private-web-server configured to store the original web-content the public-web-server provided to the private-web-server through a firewall, the private-web-server configured to

Appl. No. : **09/965,968**
Filed : **September 26, 2001**

separate the header information from a requested safe-web-file, and using the MAC (Message Authentication Code) included in the header information to check an authenticity of the safe-web-file, and the public-web-server configured to add new header information to the original web-content to create a new safe-web-file on the private-web-server computer when an unauthorized alteration of the safe-web-file is detected, wherein the new safe-web-file is sent to the public-web-server computer to automatically restore the altered safe-web-filed.

Regarding Claim 19, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 18, further comprising a real-time-check module used on the public-web-server computer for linking to an authentication module, wherein the authentication module is configured to provide authentication of the safe-web-file in response to a request received from the web visitor though http protocol.

Regarding Claim 20, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 19, wherein the real-time-check module uses a message authentication technology using chaos theory to check whether the safe-web-content has been altered.

Regarding Claim 21, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 18, wherein the real-time-check module that is configured to link the public-web-server services by using at least one message authentication technology selected from a group consisting essentially of MD4, MD5, and SHA.

Regarding Claim 22, the cited prior art does not teach or suggest an anti-alteration system for web-content having a public-web-server computer, configured to store safe-web-files which have been encrypted from original web-contents and have been provided with header information, the header information including a MAC (Message Authentication Code) generated from authentication checking the original web-content and properties including name, size, date, and storage location thereof, a private-web-server computer which retains the original web-content and which is provided to the public-web-server computer through a firewall, a real-time-check module, in response to a web visitor's request safe-web file, the real-time-check module configured to separate the a header information from the safe-web-file using a MAC (Message Authentication Code) included in the header information to authenticate the safe-web-file by comparing the header information with separate header information, and a recovery module, when an unauthorized alteration of the safe-web-file is detected, the recovery module configured to encrypt the original web-content and add header information to the original web-content to create a new safe-web-file on the private-web-

Appl. No. : **09/965,968**
Filed : **September 26, 2001**

server computer, sending the new safe-web-file to the public-web-server computer to automatically restore the safe-web-file which has been altered.

Regarding Claim 23, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 22, wherein the recovery module uses chaos encryption technology to do encryption and decryption.

Regarding Claim 24, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 22, wherein the real-time-check module is configured to provide authentication of the safe-web-file in response to a request received from the web visitor though http protocol.

Regarding Claim 25, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 23, wherein the real-time-check is configured to use a symmetric-key encryption to decrypt the safe-web-contents in response to the web visitor's request.

Regarding Claim 26, the cited prior art does not teach or suggest the anti-alteration system, recited in Claim 25, wherein the symmetric-key encryption is selected from a group consisting essentially of DES, 3DES, RC4 and AES.

Regarding Claim 27, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 24, wherein the real-time-check module uses a message authentication technology using chaos theory to check whether the safe-web-content has been altered.

Regarding Claim 28, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 24, wherein the real-time-check module uses at least one of MD4, MD5, and SHA for message authentication.

Accordingly, Applicant asserts that Claims 17-28 are allowable over the prior art, and Applicant requests allowance of Claim 17-28.

Appl. No. : 09/965,968
Filed : September 26, 2001



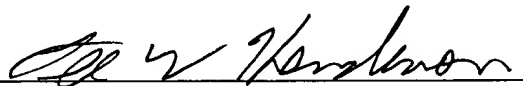
Summary

Applicant asserts that Claims 13-28 are in condition for allowance, and Applicant request allowance of Claims 13-28. If there are any remaining issues that can be resolved by a telephone conference, the Examiner is invited to call the undersigned attorney at (949) 721-6305 or at the number listed below.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: May 16, 2006

By: 

Lee W. Henderson Ph.D.

Registration No. 41,830

Attorney of Record

Customer No. 20,995

(949) 760-0404

2522466//041306